

Reduced sequences of integers and pseudo-random numbers

by

H.J.A. Duparc, C.G. Lekkerkerker and W. Peremans.

Introduction.

In this report the following two sequences of non-negative integers u_0, u_1, \dots are considered:

I. The sequences defined by

$$u_0 = b, \quad u_{n+1} = au_n \quad (n = 0, 1, \dots)$$

where a and b are positive integers.

II. The sequence of Fibonacci, defined by

$$u_0 = 0, \quad u_1 = 1; \quad u_{n+2} = u_{n+1} + u_n \quad (n = 0, 1, \dots).$$

These sequences have the property that if m is a positive integer (where in case I the number m is supposed prime to a) the least non-negative residues mod m of the elements form a periodic sequence. The length of the period of this sequence will be denoted by $C(m)$. In the case of sequence I with $a=23$, $b=47594118$ and $m=10^8+1$, Lehmer¹⁾ used the least non-negative residues of $u_0, \dots, u_{C(m)-1}$ to construct a set of pseudo-random numbers.

Our purpose is to investigate properties of the number $C(m)$. In case I we consider primes p with $(a, p) = (b, p) = 1$. Then for $p=2$ there exists a positive integer $k=k(2)$, such that

$$2^k \mid a^{C(4)} - 1, \quad 2^{k+1} \nmid a^{C(4)} - 1$$

and for odd p there exists a positive integer $k=k(p)$ such that

$$p^k \mid a^{C(p)} - 1, \quad p^{k+1} \nmid a^{C(p)} - 1.$$

In case I the following relations hold:

$$C(2) = 1;$$

$$C(p) \mid p-1;$$

$$C(2^h) = \begin{cases} C(4) & \text{if } 2 \leq h < k(2); \\ 2^{h-k(2)} C(4) & \text{if } h \geq k(2); \end{cases}$$

$$C(p^h) = \begin{cases} C(p) & \text{if } 1 \leq h < k(p); \\ p^{h-k(p)} C(p) & \text{if } h \geq k(p). \end{cases}$$

1) D.H. Lehmer, Mathematical methods in large scale computing units, Proc. Sec. Symp. on large-scale digital calculating machinery, Q 51, Harvard 141-6.

In case II for odd primes p there exists a positive integer $k=k(p)$ such that

$$p^k \mid u_{C(p)}, \quad p^k \mid u_{C(p)-1} - 1,$$

but p^{k+1} does not divide both numbers $u_{C(p)}$ and $u_{C(p)-1} - 1$. Then for sequence II we prove the following results

$$\begin{aligned} C(p) &\mid p-1 \text{ if } p \equiv \pm 1 \pmod{10}; \\ C(p) &\nmid \frac{1}{2}(p-1) \text{ if } p \equiv 11 \text{ or } 19 \pmod{20}; \\ C(p) &\mid 2(p+1) \text{ and } C(p) \nmid p+1 \text{ if } p \equiv \pm 3 \pmod{10}; \\ C(2) &= 3; \quad C(5) = 20; \\ C(2^h) &= 3 \cdot 2^{h-1} \text{ if } h \geq 1; \\ C(p^h) &= \begin{cases} C(p) & \text{if } 1 \leq h < k(p); \\ p^{h-k(p)} C(p) & \text{if } h \geq k(p). \end{cases} \end{aligned}$$

In both cases I and II if $m = p_1^{r_1} \dots p_s^{r_s}$, where p_1, \dots, p_s are different primes, the value $C(m)$ is the least common multiple of the values $C(p_i^{r_i})$ ($i=1, \dots, s$).

Special attention is given to the cases

$$m = 2^h, \quad 2^h - 1, \quad 2^h + 1, \quad 10^h, \quad 10^h - 1 \text{ and } 10^h + 1.$$

Apart from the number $C(m)$ we also define the number $c(m)$. This number $c(m)$ is the least positive integer n with $m \mid u_n$. The set of indices n with $m \mid u_n$ consists of the non-negative multiples of the number $c(m)$. In case II $c(m)$ is not necessarily equal to $C(m)$. We also deduce properties of $c(m)$ and $v(m) = \frac{C(m)}{c(m)}$.

In another report²⁾ similar properties are deduced for sequences satisfying

$$u_{n+2} = au_{n+1} + bu_n \quad (n=0, 1, \dots)$$

with arbitrary a, b, u_0 and u_1 .

§1. The sequences I.

Let a and b be positive integers and let p be a prime with $p \nmid ab$. Then there exists a positive integer n such that $a^n \equiv 1 \pmod{p}$; in fact, on account of Fermat's theorem, $n=p-1$ has this property.

Let $C(p)$ be the smallest positive integer with this property. Then, if $m \equiv n \pmod{C(p)}$, we have $ba^m \equiv ba^n \pmod{p}$ and conversely. This proves that the sequence of numbers $u_n = ba^n$ ($n=0, 1, \dots$) is periodic mod p with period $C(p)$.

From Fermat's theorem it follows further

$$(1, 1) \quad C(p) \mid p-1.$$

In view of the application of the sequences I to the construction of pseudo-random numbers it is required that $C(p)$ be large.

If p is an odd prime and if $a^t \equiv 1 \pmod{p^j}$, $a^t \not\equiv 1 \pmod{p^{j+1}}$, where t and j are positive integers, then $a^{pt} \equiv 1 \pmod{p^{j+1}}$, $a^{pt} \not\equiv 1 \pmod{p^{j+2}}$. This property remains valid if $p=2$ supposed $j \geq 2$. Herefrom follow the relations (1) and (2).

From Euler's theorem $a^{\varphi(m)} \equiv 1 \pmod{m}$ it follows $C(p^s) \mid \varphi(p^s)$. The value of $C(m)$ for arbitrary $m=p_1^{r_1} \dots p_s^{r_s}$, where p_1, \dots, p_s are different primes, is obviously a common multiple of the numbers $C(p_i^{r_i})$ ($i=1, \dots, s$), hence the least common multiple. Hence for all a with $(a, m)=1$ the number $C(m)$ divides the least common multiple $L(m)$ of the numbers $\varphi(p_i^{r_i})$ ($i=1, \dots, s$).

We give a table of the value of $L(m)$ for $m=10^n-1$ ($n=1, 2, \dots$).

n	$m=10^n-1$	$\varphi(p_i^{r_i})$	$L(m)$
1	3^2	6	6
2	$3^2.11$	6; 10	30
3	$3^3.37$	18; 36	36
4	$3^2.101$	6; 100	300
5	$3^2.41.271$	6; 40; 270	1080
6	$3^3.7.11.13.37$	18; 6; 10; 12; 36	180
7	$3^2.239.4649$	6; 238; 4648	711144
8	$3^2.73.11.101.137$	6; 72; 10; 100; 136	30600
9	$3^4.37.333667$	54; 36; 333666	667332
10	$3^2.11.41.271.9091$	6; 10; 40; 270; 9090	109080

From the table we learn that $L(m)$ is much smaller than m , if the number of prime factors in n is not too small. In fact the numbers p_i-1 ($i=1, \dots, s$) have at least a factor 2 in common, so

$$L(m) < \frac{\varphi(m)}{2^{s-1}} < \frac{m}{2^{s-1}}.$$

We give a similar table for $m=10^n+1$.

n	$m=10^n+1$	$\varphi(p_i^{r_i})$	$L(m)$
1	11	10	10
2	101	100	100
3	7.11.13	6; 10; 12	60
4	73.137	72.136	1224
5	11.9091	10; 9090	9090
6	101.9901	100; 9900	9900
7	11.909091	10; 909090	909090

The prime factors which occur in the first table in the $2n^{\text{th}}$ row and not earlier, are the same as the prime factors which occur in the second table in the n^{th} row and not earlier. This follows from the following considerations

- 1°. Let p be a prime with $p \mid 10^{2n}-1$, $p \nmid 10^h-1$ for $0 < h < 2n$. From $p \mid (10^n+1)(10^n-1)$ and $p \nmid 10^n-1$ it follows $p \mid 10^n+1$. If $0 < k < n$, then from $p \nmid 10^{2k}-1$ it follows $p \nmid 10^k+1$.
- 2°. Let p be a prime with $p \mid 10^n+1$, $p \nmid 10^k+1$ with $0 < k < n$. Then $p \mid 10^{n+1} \mid 10^{2n}-1$. Should a number h exist such that $0 < h < 2n$ and $p \mid 10^h-1$, then it would follow $10^{h-n} \equiv -1 \pmod{p}$ and $10^{n-h} \equiv -1 \pmod{p}$ hence $10^{|n-h|} \equiv -1 \pmod{p}$, where $0 < |n-h| < n$, contrary to the assumption on k . Hence $p \nmid 10^h-1$ if $0 < h < 2n$.

It is well known that there exists a primitive root mod p^r , where p is a prime and r a positive integer, i.e. there exists an integer a with

$$a^{\varphi(p^r)} \equiv 1 \pmod{p^r}; \quad a^h \not\equiv 1 \pmod{p^r} \text{ if } 0 < h < \varphi(p^r).$$

Now suppose $m = p_1^{r_1} \dots p_s^{r_s}$, where p_1, \dots, p_s are different primes. Let a_i be a primitive root mod $p_i^{r_i}$ ($i=1, \dots, s$). On account of the chinese remainder theorem there exists a number a such that $a \equiv_{r_i} a_i \pmod{p_i^{r_i}}$ ($i=1, \dots, s$). Each common multiple h of the numbers $\varphi(p_i^{r_i})$ ($i=1, \dots, s$) satisfies $a^h \equiv 1 \pmod{m}$ and conversely. Hence for this choice of a the number $C(m)$ is equal to the least common multiple $L(m)$ of the numbers $\varphi(p_i^{r_i})$ ($i=1, \dots, s$).

Since above we found $C(m) \mid L(m)$, we now have the following result. If m is fixed and a is variable, the greatest value attained by $C(m)$ is $L(m)$. For instance $C(m)=L(m)$ if we take for a the above constructed number.

Example. If $m=10^5-1$ and $a=7$, then $C(m)=L(m)=1080=2^3 3^3 5$. For

$$C(m) \nmid \frac{1}{2} \cdot 1080 \text{ since } 7^{540} \equiv -1 \pmod{41};$$

$$C(m) \nmid \frac{1}{5} \cdot 1080 \text{ since } 7^{360} \equiv -29 \pmod{271};$$

$$C(m) \nmid \frac{1}{5} \cdot 1080 \text{ since } 7^{216} \equiv 16 \pmod{41}.$$

Although for $a=7$ we have $C(3^2) \neq \varphi(3^2)$, still $C(m)=L(m)$. The number $a=7$ is the smallest number for which $C(m)=L(m)$, for if $a=2$ we have $2^{20} \equiv 1 \pmod{41}$ hence $C(m) \mid \frac{1}{2} L(m)$; if $a=4$ we then also have $C(m) \mid \frac{1}{2} L(m)$; if $a=5$ we have $5^{20} \equiv 1 \pmod{41}$, hence $C(m) \mid \frac{1}{2} L(m)$. The values $a=3$ and $a=6$ are excluded since $(3, m) = (6, m) = 3 \neq 1$.

For computing machines working in the binary scale the reduction mod m of integers is simple in the cases $m=2^n-1$, $m=2^n+1$, $m=2^n$. We therefore give also tables of $L(m)$ for $m=2^n-1$ and $m=2^n+1$.

n	$m=2^n-1$	$\varphi(p_i^{s_i})$	L(m)
2	3	2	2
3	7	6	6
4	3.5	2;4	4
5	31	30	30
6	$3^2.7$	6;6	6
7	127	126	126
8	3.5.17	2;4;16	16
9	7.73	6;72	72
10	3.11.31	2;10;30	30
11	23.89	22;88	88
12	$3^2.5.7.13$	6;4;6;12	12
13	8191	8190	8190
14	3.43.127	2;42;126	126
15	7.31.151	6;30;150	150
16	3.5.17.257	2;4;16;256	256
...
29	233.1103.2089	232;1102;2088	39672
30	$3^2.7.11.31.151.331$	6;6;10;30;150;330	1650

n	$m=2^n+1$	$\varphi(p_i^{s_i})$	L(m)
1	3	2	2
2	5	4	4
3	3^2	6	6
4	17	16	16
5	3.11	2;10	10
6	5.13	4;12	12
7	3.43	2;42	42
8	257	256	256
9	$3^3.19$	18;18	18
10	$5^2.41$	20;40	40
11	3.683	2;682	682
12	17.241	16;240	240
13	3.2731	2;2730	2730
14	5.29.113	4;28;112	112
15	$3^2.11.331$	6;10;330	330
16	65537	65536	65536
...
29	3.59.3033169	2;58;3033168	3033168
30	$5^2.13.41.61.1321$	20;12;40;60;1320	1320

For the ARRA³⁾ especially reduction mod m where $m=2^{30}+1$ is simple. In these cases however the value of $L(m)$ is not large. Now $L(m)$ has a greater value if $m=2^{29}+1$, whereas the reduction mod $2^{29}+1$ is still relatively simple.

If $m=2^{29}-1=233.1103.2089$, then $L(m)$ is the least common multiple $2^3.3^2.19.29$ of $232=2^3.29$, $1102=2.19.29$, $2088=2^3.3^2.29$. If we take $a=3$, then $C(m)=L(m)=2^3.3^2.19.29=39672$. For

$C(m) \nmid \frac{1}{2}.39672$ since $3^{116} \equiv -1 \pmod{233}$;

$C(m) \nmid \frac{1}{3}.39672$, since if $3^{13224} \equiv 1 \pmod{2089}$ we would get from $3^{2088} \equiv 1 \pmod{2089}$ that $3^{696} \equiv 1 \pmod{2089}$ which contradicts $3^{696} \equiv 826 \pmod{2089}$;

$C(m) \nmid \frac{1}{19}.39672$, since if $3^{2088} \equiv 1 \pmod{1103}$ we would get from $3^{1102} \equiv 1 \pmod{1103}$ that $3^{58} \equiv 1 \pmod{1103}$, which contradicts $3^{58} \equiv 620 \pmod{1103}$;

$C(m) \nmid \frac{1}{29}.39672$, since if $3^{1368} \equiv 1 \pmod{233}$ we would get from $3^{232} \equiv 1 \pmod{233}$ that $3^8 \equiv 1 \pmod{233}$, which contradicts $3^8 \equiv 37 \pmod{233}$.

If $m=2^{29}+1=3.59.3033169$, then $L(m)$ is the least common multiple $2^4.3.29.2179$ of $2, 58=2.29$ and $3033168=2^4.3.29.2179$. Here $a=2$ has the period $C(m)=58$, so $a=4$ has the period 29, whereas $a=3$ and $a=6$ are excluded since $(3, m) = (6, m) = 3 \neq 1$. Since $5^{\frac{1}{2}.3033168} \equiv 1 \pmod{3033169}$ also for $a=5$ we have $C(m) < L(m)$. For $a=7$ however $C(m)=L(m)=3033168$, for

$C(m) \nmid \frac{1}{2}.3033168$, since $7^{1532584} \equiv -1 \pmod{3033169}$;

$C(m) \nmid \frac{1}{3}.3033168$, since $7^{1011056} \equiv 1554651 \pmod{3033169}$;

$C(m) \nmid \frac{1}{29}.3033168$, since if $7^{14592} \equiv 1 \pmod{59}$ we would get from $7^{58} \equiv 1 \pmod{59}$ that $7^2 \equiv 1 \pmod{59}$ contrary to $7^2 \equiv 49 \pmod{59}$;

$C(m) \nmid \frac{1}{2179}.3033168$, since $7^{1292} \equiv 1511637 \pmod{3033169}$.

In order to find $C(m)$ if $m=2^n$, we remark that $C(4)=1$ if $a \equiv 1 \pmod{4}$ and $C(4)=2$ if $a \equiv 3 \pmod{4}$; in the latter case the integer k defined in the introduction is ≥ 3 . We also give a table of the values of $C(2^h)$ ($h \geq k$) for the odd integers a .

a	$C(4)$	k	$C(2^h)$
3	2	3	2^{h-2}
5	1	2	2^{h-2}
7	2	4	2^{h-3}
9	1	3	2^{h-3}
11	1	3	2^{h-3}
13	1	2	2^{h-2}
15	2	5	2^{h-4}
17	1	4	2^{h-4}
19	2	3	2^{h-2}
21	1	2	2^{h-2}

3) ARRA = Automatische Relais Rekenmachine Amsterdam
(Automatic Relay Computer Amsterdam)

§2. The sequence II.

We now investigate the sequence of Fibonacci defined by

$$u_0=0, u_1=1; u_{n+2}=u_{n+1}+u_n \quad (n=0,1,\dots).$$

Let ω and $\bar{\omega}$ be the roots of the equation

$$x^2-x-1=0,$$

with $\omega > \bar{\omega}$. Then we have

$$(1) \quad \sqrt{5}=2\omega-1; \omega^2=\omega+1; \frac{1}{\omega}=\omega-1; \omega+\bar{\omega}=1; \omega\bar{\omega}=-1;$$

$$(2) \quad \omega^n = u_n \omega + u_{n-1}; \bar{\omega}^n = u_n \bar{\omega} + u_{n-1} \quad (n=1,2,\dots);$$

$$(3) \quad u_n = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} \quad (n=0,1,\dots);$$

$$(4) \quad u_{2n-1} = u_n^2 + u_{n-1}^2; u_{2n} = u_n(u_{n+1} + u_{n-1}) \quad (n=1,2,\dots);$$

$$(5) \quad u_n | u_m \quad \text{if} \quad n | m.$$

Formulae (1) are obvious; formulae (2) are proved by mathematical induction, while (3) follows from (2). Further from (1) and (2) follows

$$u_{2n}\omega + u_{2n-1} = \omega^{2n} = (u_n\omega + u_{n-1})^2 = (u_n^2 + 2u_n u_{n-1})\omega + u_n^2 + u_{n-1}^2,$$

whence follows (4) by the irrationality of ω .

From $n|m$ and (3) it follows that $\frac{u_m}{u_n}$ is a polynomial in ω^n and $\bar{\omega}^n$ with integral coefficients which using the formulae (2) and (1), can be written in the form $a\omega + b$ where a and b are integral. Since $\frac{u_m}{u_n}$ is rational and ω is irrational we get $a=0$, whence follows (5).

We define $a\omega + b \equiv c\omega + d \pmod{m}$ by $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. If $a\omega + b \equiv 0 \pmod{m}$ we also write $m | a\omega + b$.

Theorem 1. Let m be an arbitrary positive integer and let $c=c(m)$ be the smallest positive integer with $u_c \equiv 0 \pmod{m}$. Then $u_d \equiv 0 \pmod{m}$ if and only if $d \geq 0$, $c | d$.

Proof. Let d be a non negative integer. If $c | d$ from (5) follows $u_c | u_d$. If conversely $u_d \equiv 0 \pmod{m}$, put $d=qc+r$ where $0 \leq r \leq c-1$. Then

$$\omega^d = u_d \omega + u_{d-1} \equiv u_{d-1} \pmod{m}$$

and

$$\bar{\omega}^{qc} = (u_c \bar{\omega} + u_{c-1})^q \equiv u_{c-1}^q \pmod{m},$$

hence

$$\omega^r = \omega^{d-qc} = \omega^d (-\bar{\omega})^{qc} \equiv (-)^{qc} u_{d-1} u_{c-1}^q \pmod{m},$$

whence follows $u_r \equiv 0 \pmod{m}$, so $r=0$ and $c | d$.

Corollary. If $m | n$, then we have $u_{c(n)} \equiv 0 \pmod{m}$, hence by the last theorem $c(m) | c(n)$.

Theorem 2. Let m be an arbitrary positive integer and let $C=C(m)$ be the smallest positive integer with

$$\omega^C \equiv 1 \pmod{m}, \text{ i.e. } u_C \equiv 0 \pmod{m}, u_{C-1} \equiv 1 \pmod{m}.$$

Then for d non negative $\omega^d \equiv 1 \pmod{m}$ if and only if $C | d$.

Proof. Let d be a non negative integer. If $C | d$ from $\omega^C \equiv 1 \pmod{m}$ follows $\omega^d \equiv 1 \pmod{m}$. If conversely $\omega^d \equiv 1 \pmod{m}$, put $d=qC+r$, where

$0 \leq r \leq C-1$. Then $1 \equiv \omega^d = \omega^{qC} \omega^r \equiv \omega^r \pmod{m}$, whence follows $r=0$ and $C \mid d$.
Corollary. If $m \mid n$, then we have $\omega^{C(n)} \equiv 1 \pmod{m}$, hence by the last theorem $C(m) \mid C(n)$.

We put $v = v(m) = \frac{C(m)}{c(m)}$. For this number we prove

Theorem 3. For every m the number $v(m)$ is integral and $v(m)$ is the smallest exponent satisfying

$$u_{C-1}^v \equiv 1 \pmod{m}.$$

Proof. From theorem 1 it follows $c(m) \mid C(m)$, hence v is integral.

Since $\omega^C \equiv u_{C-1} \pmod{m}$, we have

$$1 \equiv \omega^C = (\omega^C)^v \equiv u_{C-1}^v \pmod{m}.$$

Further there does not exist a number w with $u_{C-1}^w \equiv 1 \pmod{m}$ and $0 < w < v$, for otherwise we would have

$$\omega^{cw} \equiv u_{C-1}^w \equiv 1 \pmod{m},$$

with $0 < cw < C$, contrary to the definition of C .

Theorem 4. If $c(m)$ is even then $v=1$ or 2 ; if $c(m)$ is odd then $v=4$.

Proof. From $\omega^C \equiv u_{C-1} \pmod{m}$ and $\bar{\omega}^C \equiv u_{C-1} \pmod{m}$, it follows

$$(-)^C \equiv (\omega \bar{\omega})^C \equiv u_{C-1}^2 \pmod{m}.$$

If c is even the preceding theorem learns $v \mid 2$. If c is odd we have $u_{C-1}^2 \equiv -1 \pmod{m}$ and $u_{C-1}^4 \equiv 1 \pmod{m}$, hence $v=4$.

Theorem 5. If p is a prime we have

$$\begin{aligned} c(p) &\mid p-1 && \text{if } p \equiv \pm 1 \pmod{10}; \\ c(p) &\mid \frac{1}{2}(p-1) && \text{if } p \equiv 1 \text{ or } 9 \pmod{20}; \\ c(p) &\nmid \frac{1}{2}(p-1) && \text{if } p \equiv 11 \text{ or } 19 \pmod{20}; \\ c(p) &\mid p+1 && \text{if } p \equiv \pm 3 \pmod{10}; \\ c(p) &\nmid \frac{1}{2}(p+1) && \text{if } p \equiv 3 \text{ or } 7 \pmod{20}; \\ c(p) &\mid \frac{1}{2}(p+1) && \text{if } p \equiv 13 \text{ or } 17 \pmod{20}; \\ c(2) &= 3; \quad c(5) = 5; \\ C(p) &\mid p-1 && \text{if } p \equiv \pm 1 \pmod{10}; \\ C(p) &\nmid \frac{1}{2}(p-1) && \text{if } p \equiv 11 \text{ or } 19 \pmod{20}; \\ C(p) &\mid 2(p+1), C(p) \nmid p+1 && \text{if } p \equiv \pm 3 \pmod{10}; \\ C(2) &= 3; \quad C(5) = 20. \end{aligned}$$

Proof. We shall treat the cases $p \equiv \pm 1 \pmod{10}$ and $p \equiv \pm 3 \pmod{10}$ separately.

A. $p \equiv \pm 1 \pmod{10}$. By the theory of quadratic residues we have $5^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$, hence

$$(2\omega - 1)^{p-1} \equiv 1 \pmod{p}, \quad (2\omega - 1)^p \equiv 2\omega - 1 \pmod{p},$$

$$2^p \omega^{p-1} \equiv 2\omega - 1 \pmod{p}, \quad 2\omega^p \equiv 2\omega \pmod{p},$$

whence after multiplication by $\frac{1}{2}(p-1)\bar{\omega}$ we get $\omega^{p-1} \equiv 1 \pmod{p}$, so $c \mid C \mid p-1$ by theorem 2 and 3.

A1. $p \equiv 1$ or $9 \pmod{20}$. Since in this case -1 is a quadratic residue mod p , there exists an integer k with $k^2 \equiv -1 \pmod{p}$. We have $k \not\equiv 2 \pmod{p}$ for otherwise we should have $p \mid 5$.

From $\omega^2 - 1 = \omega$ it follows

$$\begin{aligned}\omega^2 + k^2 &\equiv \omega \pmod{p}, & (\omega + k)^2 &\equiv \omega(1 + 2k) \pmod{p}, \\ (\omega + k)^{p-1} &\equiv \omega^{\frac{1}{2}(p-1)} (1 + 2k)^{\frac{1}{2}(p-1)} \pmod{p}, \\ (\omega + k)^p &\equiv \omega^{\frac{1}{2}(p-1)} (1 + 2k)^{\frac{1}{2}(p-1)} (\omega + k) \pmod{p}.\end{aligned}$$

For the left hand member we have

$$(\omega + k)^p \equiv \omega^p + k^p \equiv \omega + k \pmod{p},$$

hence after multiplication by $(\bar{\omega} + k)(k - 2)^{-1}$, on account of $(\omega + k)(\bar{\omega} + k) = -k^2 + k - 1 \equiv k - 2 \pmod{p}$, we get

$$1 \equiv \omega^{\frac{1}{2}(p-1)} (1 + 2k)^{\frac{1}{2}(p-1)} \pmod{p},$$

hence

$$\omega^{\frac{1}{2}(p-1)} \equiv (1 + 2k)^{\frac{1}{2}(p-1)} \pmod{p}.$$

So we have proved $c(p) \mid \frac{1}{2}(p-1)$.

A2. $p \equiv 11$ or $19 \pmod{20}$. Suppose $c \mid \frac{1}{2}(p-1)$. Then a rational integer exists with $\omega^{\frac{1}{2}(p-1)} \equiv r \pmod{p}$, hence also $\bar{\omega}^{\frac{1}{2}(p-1)} \equiv r \pmod{p}$. After multiplication we obtain in view of (1) and of $p \equiv 3 \pmod{4}$

$$r^2 \equiv \omega^{\frac{1}{2}(p-1)} \bar{\omega}^{\frac{1}{2}(p-1)} = -1 \pmod{p}.$$

Hence -1 is a quadratic residue mod p , contrary to $p \equiv 3 \pmod{4}$. So we proved $c \nmid \frac{1}{2}(p-1)$, hence a fortiori $C \nmid \frac{1}{2}(p-1)$.

B. $p \equiv \pm 3 \pmod{10}$. By the theory of quadratic residues we have $5^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$, hence

$$\begin{aligned}(2\omega - 1)^{p-1} &\equiv -1 \pmod{p}, & (2\omega - 1)^p &\equiv 1 - 2\omega \pmod{p}, \\ 2^p \omega^{p-1} &\equiv 1 - 2\omega \pmod{p}, & \omega^p &\equiv 1 - \omega \pmod{p}.\end{aligned}$$

After multiplication by ω we get

$$\omega^{p+1} \equiv \omega - \omega^2 = -1 \pmod{p},$$

so $c(p) \mid p+1$, $C(p) \nmid p+1$. Finally by squaring the last congruence we find

$$\omega^{2(p+1)} \equiv 1 \pmod{p},$$

hence

$$C(p) \mid 2(p+1).$$

B1. $p \equiv 3$ or $7 \pmod{20}$. Suppose $c \mid \frac{1}{2}(p+1)$. Then a rational integer r exists with $\omega^{\frac{1}{2}(p+1)} \equiv r \pmod{p}$, hence also $\bar{\omega}^{\frac{1}{2}(p+1)} \equiv r \pmod{p}$. So $\omega^{\frac{1}{2}(p+1)} \equiv \bar{\omega}^{\frac{1}{2}(p+1)} \pmod{p}$. After multiplication by $\omega^{\frac{1}{2}(p+1)}$ we get

$$\omega^{p+1} \equiv (\omega \bar{\omega})^{\frac{1}{2}(p+1)} = 1 \pmod{p},$$

contrary to $C(p) \nmid p+1$. Hence $c \nmid \frac{1}{2}(p+1)$.

B2. $p \equiv 13$ or $17 \pmod{20}$. As in case A1 there exists an integer k with $k^2 \equiv -1 \pmod{p}$. Now from

$$(\omega + k)^2 \equiv \omega(1 + 2k) \pmod{p}$$

we deduce

$$(\omega + k)^{p+1} \equiv \omega^{\frac{1}{2}(p+1)} (1 + 2k)^{\frac{1}{2}(p+1)} \pmod{p}.$$

Using the result $\omega^p \equiv 1 - \omega = \bar{\omega} \pmod{p}$ found in B, we have

$$(\omega + k)^{p+1} \equiv (\omega + k)(\omega^p + k) \equiv (\omega + k)(\bar{\omega} + k) \equiv k - 2 \pmod{p}.$$

We remark that $1 + 2k \not\equiv 0 \pmod{p}$, for otherwise we would have

$$k - 2 \equiv \omega^{\frac{1}{2}(p+1)}(1 + 2k)^{\frac{1}{2}(p+1)} \equiv 0 \pmod{p}.$$

Hence

$$\omega^{\frac{1}{2}(p+1)} \equiv (k - 2)(1 + 2k)^{\frac{1}{2}(p-3)} \pmod{p},$$

so

$$c(p) \mid \frac{1}{2}(p+1).$$

The values of $c(2)$, $c(5)$, $c(2)$ and $c(5)$ easily follow from the table of Fibonacci numbers. The relation $C(5) = 4c(5)$ is in accordance with theorem 4.

Theorem 6. If p is a prime > 2 , and if $k(p)$ is the greatest integer with

$$p^{k(p)} \mid \omega^{C(p)} - 1,$$

and if h is a positive integer, then

$$C(p^h) = \begin{cases} C(p) & \text{if } 1 \leq h \leq k(p); \\ p^{h-k(p)} C(p) & \text{if } h \geq k(p). \end{cases}$$

Remark. By definition we have $\omega^{C(p)} \equiv 1 \pmod{p}$, hence $k(p)$ is a positive integer.

Proof. Suppose $1 \leq h \leq k(p)$. Then we have $\omega^{C(p)} \equiv 1 \pmod{p^h}$. Further if t is a positive integer $< C(p)$, then $\omega^t \not\equiv 1 \pmod{p}$, hence $\omega^t \not\equiv 1 \pmod{p^h}$. So in view of the definition of $C(m)$ we have $C(p^h) = C(p)$.

Now suppose $h \geq k(p)$. By induction we simultaneously prove the following three relations

$$(6) \quad \omega^{C(p^h)} \equiv 1 \pmod{p^h}; \quad \omega^{C(p^h)} \not\equiv 1 \pmod{p^{h+1}}; \quad C(p^h) = p^{h-k(p)} C(p);$$

the third relation is the required result. For $h = k(p)$ these relations hold in view of the definition of $k(p)$ and the first part of the theorem. Now suppose the relations (6) hold for an integer $h \geq k(p)$. Then from the first and the second relation (6) follows

$$\omega^{C(p^h)} = 1 + p^h a,$$

where $a = a_1 \omega + a_2$ (a_1, a_2 integral) is not divisible by p . Hence

$$\omega^{pC(p^h)} = (1 + p^h a)^p \equiv 1 + p^{h+1} a \pmod{p^{h+2}},$$

so

$$(7) \quad \omega^{pC(p^h)} \equiv 1 \pmod{p^{h+1}}; \quad \omega^{pC(p^h)} \not\equiv 1 \pmod{p^{h+2}}.$$

Thus by theorem 2 we have $C(p^{h+1}) \mid pC(p^h)$. From the second relation (6) follows $C(p^{h+1}) \nmid C(p^h)$ and by the corollary of theorem 2 we have $C(p^h) \mid C(p^{h+1})$. These three relations involve

$$(8) \quad C(p^{h+1}) = pC(p^h).$$

Hence the three relations (6) hold with $h+1$ instead of h , the first and second by (7) and (8), the third by (8) and the induction hypothesis.

Theorem 7. If p is a prime > 2 , if $k(p)$ is the integer defined in theorem 6 and if h is a positive integer, then

$$c(p^h) = \begin{cases} c(p) & \text{if } 1 \leq h \leq k(p); \\ p^{h-k(p)} c(p) & \text{if } h \geq k(p). \end{cases}$$

Proof. By theorem 6 there exists a non negative integer s , such that $C(p^h) = p^s C(p)$. A similar property holds for $c(p^h)$.

First by the corollary of theorem 1 we have $c(p) \mid c(p^h)$. Further we have $\omega^{c(p)} \equiv r \pmod{p}$, where r is a rational integer. So we can write $\omega^{c(p)} = r + ap$, where $a = a_1 \omega + a_2$ with integral a_1, a_2 . Hence

$$\omega^{p^{h-1} c(p)} = (r + ap)^{p^{h-1}} \equiv r^{p^{h-1}} \pmod{p^h},$$

thus by theorem 1 we have $c(p^h) \mid p^{h-1} c(p)$. Hence we infer the existence of a non negative integer t with

$$c(p^h) = p^t c(p).$$

We then have

$$v(p^h) = \frac{C(p^h)}{c(p^h)} = \frac{p^s C(p)}{p^t c(p)} = p^{s-t} v(p).$$

Since by theorem 4 the quotient $v(m)$ assumes the values 1, 2 or 4 only we have $p^{s-t} = \frac{v(p^h)}{v(p)} = 1$, hence $s=t$. Then from theorem 6 follows the assertion.

Theorem 8. For integers $h \geq 3$ we have

$$C(2^h) = 2c(2^h) = 3 \cdot 2^{h-1}.$$

Further

$$C(2) = c(2) = 3; \quad C(4) = c(4) = 6.$$

Proof. From the table it follows that $C(2) = c(2) = 3$, $C(4) = c(4) = 6$. For integers $h \geq 2$ we have

$$\omega^{C(2^h)} \equiv 1 \pmod{2^h}; \quad \omega^{C(2^h)} \not\equiv 1 \pmod{2^{h+1}}; \quad C(2^h) = 3 \cdot 2^{h-1}.$$

These relations are proved by induction in entirely the same way as the relations (6) in theorem 6.

Now suppose $h \geq 3$ in theorem 6. By our last result we have

$$\omega^{\frac{1}{2}C(2^h)} = \omega^{C(2^{h-1})} \equiv 1 \pmod{2^{h-1}},$$

so we can write

$$\omega^{\frac{1}{2}C(2^h)} = 1 + (a + b\omega)2^{h-1},$$

where a and b are rational integers. Multiplying this relation by its conjugate we get on account of (1) and $2 \mid \frac{1}{2}C(2^h)$

$$1 = (\omega \bar{\omega})^{\frac{1}{2}C(2^h)} = 1 + (2a + b)2^{h-1} + (a^2 + ab - b^2)2^{h-2} \equiv 1 + b \cdot 2^{h-1} \pmod{2^h}$$

Hence b is even, so we have

$$\omega^{\frac{1}{2}C(2^h)} \equiv 1 + a \cdot 2^{h-1} \pmod{2^h}.$$

Since a is a rational integer by theorem 1 we conclude

$$c(2^h) \mid \frac{1}{2}C(2^h).$$

Since $c(4)$ is even, by the corollary of theorem 1 also $c(2^h)$ is even, hence by theorem 4 we have $v(2^h)=1$ or 2 . Combining this with the last relation we conclude $v(2^h)=2$, $c(2^h)=\frac{1}{2}C(2^h)$.

Theorem 9. If $m=p_1^{r_1} \dots p_s^{r_s}$, where p_1, \dots, p_s are different primes, then $c(m)$ is the least common multiple of the numbers $c(p_i^{r_i})$ and $C(m)$ is the least common multiple of the numbers $C(p_i^{r_i})$ ($i=1, \dots, s$).

Proof. By the corollary of theorem 1 we have

$$c(p_i^{r_i}) \mid c(m) \quad (i=1, \dots, s).$$

Further if g is the least common multiple of the s numbers $c(p_i^{r_i})$ ($i=1, \dots, s$) then by theorem 1

$$u_g \equiv 0 \pmod{p_i^{r_i}} \quad (i=1, \dots, s),$$

hence $u_g \equiv 0 \pmod{m}$. Again by theorem 1 we get $c(m) \mid g$. Hence $c(m)=g$.

Using the theorem 2 instead of theorem 1 we find in a similar way the result for $C(m)$.

If p is prime and $c(p)$ is even we have the following amelioration of theorem 4:

Theorem 10. If $c(p) \equiv 0 \pmod{4}$ then $v=2$;
if $c(p) \equiv 2 \pmod{4}$ then $v=1$.

Proof. We put $c(p)=2d$. Then we have

$$\omega^{2d} \equiv u_{c-1} \pmod{p},$$

hence after multiplication by $\bar{\omega}^d$ we get from (1)

$$(-)^d \omega^d \equiv u_{c-1} \bar{\omega}^d \pmod{p}.$$

Since $d < c(p)$ we have $u_d \not\equiv 0 \pmod{p}$, hence $\omega^d \not\equiv \bar{\omega}^d \pmod{p}$. Thus $u_{c-1} \not\equiv (-)^d \pmod{p}$. From theorem 4 follows $u_{c-1}^2 \equiv 1 \pmod{p}$, hence $u_{c-1} \equiv \pm 1 \pmod{p}$. If $c(p) \equiv 0 \pmod{4}$, the integer d is even, hence $u_{c-1} \equiv -1 \pmod{p}$, and $v=2$. If $c(p) \equiv 2 \pmod{4}$, the integer d is odd, hence $u_{c-1} \equiv 1 \pmod{p}$ and $v=1$.

The results concerning $v(p)$ can be listed as follows

(9)

$c(p) \pmod{4}$	± 1	2	0
$v(p)$	4	1	2

Theorem 11. If m is an arbitrary positive integer, then $v(m)=2$ apart from the following cases:

1°. if $m=2^t m_1$, where $t=0, 1$ or 2 , where m_1 is odd and $c(p) \equiv 2 \pmod{4}$ for each prime factor p of m_1 , then $v(m)=1$;

2°. if $m=2^t m_1$, where $t=0$ or 1 , where m_1 is odd and $\neq 1$, and if $c(p) \equiv \pm 1 \pmod{4}$ for each prime factor p of m_1 , then $v(m)=4$.

Proof. From the values of $c(2^h)$ and $C(2^h)$ found in theorem 8 it follows that $v(2^h) = \begin{cases} 1 & \text{if } h=1, 2; \\ 2 & \text{if } h=3, 4, \dots \end{cases}$.

Hence 1^0 is proved in the case $m_1=1$.

Now suppose $m=2^t m_1$, where m_1 is odd and $\neq 1$.

From theorems 6 and 7 it follows that for odd primes p we have

$$v(p^h)=v(p).$$

Let d_1 and D_1 be zero if $t=0$ and let d_1 and D_1 denote the number of factors 2 in $c(2^t)$ and $C(2^t)$ respectively if $t \geq 1$; let d_2 and D_2 denote the number of factors 2 in $c(m_1)$ and $C(m_1)$ respectively. Further put $d=\max(d_1, d_2)$; $D=\max(D_1, D_2)$.

Then by theorem 9 the integers d and D are equal to the numbers of factors 2 in $c(m)$ and $C(m)$ respectively. Since by theorem 4 the number $v(m)$ is a power of 2, we have the formula

$$v(m)=2^{D-d}.$$

We now consider three cases:

A. $c(p_i) \equiv \pm 1 \pmod{4}$ for each prime factor p_i of m_1 . Then by theorems 9, 7 and 4 we have $d_2=0$, $D_2=2$. Using theorem 8 we have

$$(10) \quad \begin{cases} d_1=D_1=0 & \text{if } t=0 \text{ or } 1; \\ d_1=D_1=1 & \text{if } t=2; \\ d_1=1, D_1=2 & \text{if } t=3; \\ d_1 \geq 2, D_1=d_1+1 & \text{if } t \geq 4. \end{cases}$$

Herefrom follows $D-d=2$, hence $v(m)=4$, if $t=0$ or 1; $D-d=1$, hence $v(m)=2$, if $t \geq 2$.

B. $c(p_i) \equiv 2 \pmod{4}$ for each prime factor p_i of m_1 . Then by theorems 9, 7 and 10 we have $d_2=1$, $D_2=1$. Using the relations (10) we now find $D-d=0$, hence $v(m)=1$, if $t=0, 1$ or 2; $D-d=1$, hence $v(m)=2$, if $t \geq 3$.

C. In all other cases by inspection of the table (9) we infer $d_2 \geq 1$, $D_2-d_2=1$. For instance $d_2=1$, $D_2=2$ if m_1 only contains prime factors p with $c(p) \equiv \pm 1 \pmod{4}$ and prime factors p with $c(p) \equiv 2 \pmod{4}$.

If $d_2 \geq d_1$, then by (10) we have $D_2 \geq D_1$, hence $D-d=D_2-d_2=1$, hence $v(m)=2$. If $d_2 < d_1$, then $d_1 \geq 2$, hence by (10) we get $D_1-d_1=1$, so $D-d=1$, $v(m)=2$. This proves the theorem.

It is not without interest to apply the above theorems the problem of factorizing the elements of the sequence II of Fibonacci treated by E. Lucas⁴⁾, D. Jarden⁵⁾ and A. Katz⁵⁾.

From (5) it follows that u_n is divisible by all the numbers u_d where $d|n$. In view of this fact we call a prime factor of u_d with $d|n$

4) E. Lucas. Théorie des fonctions numériques simplement périodiques, Amer. Journ. of Math. 1 (1878), 184-240, 289-321.

5) D. Jarden and A. Katz wrote about ten papers on this subject in Riveon Lematematika 1-4(1946-1950).

and $1 < d < n$ a trivial prime factor of u_n . The largest divisor of u_n which only contains trivial prime factors of u_n will be called the trivial divisor of u_n .

Suppose $n = p_1^{r_1} \dots p_s^{r_s}$, where p_1, \dots, p_s are different prime factors. Put $n_i = \frac{n}{p_i^{r_i}}$ ($i=1, \dots, s$). Then the set of trivial prime factors of u_n is the set of prime factors of n_i ($i=1, \dots, s$). Determining the highest powers of the trivial prime factors which divide u_n , we find that the trivial divisor of u_n is equal to the least common multiple of the s numbers

$$p_i^{\varepsilon_i} u_{n_i} \quad (i=1, \dots, s),$$

where $\varepsilon_i = 1$ if $p_i \mid u_{n_i}$ and $\varepsilon_i = 0$ if $p_i \nmid u_{n_i}$ ($i=1, \dots, s$).

The factorization of u_n in practice reduces to the determination of the non trivial prime factors of u_n . In another report we shall prove that apart from the cases $n=1, 2, 6$ and 12 the number u_n contains non trivial prime factors.

Now if p is a non trivial prime factor of u_n then in view of theorem 1, we have $c(p)=n$. So considering successively the cases $p \equiv 1, 9, 3, 7 \pmod{10}$ by theorem 5, it is required for a prime p to be a non trivial prime factor of u_n , that there exists a positive integer x such that

$$p = xn + 1, \text{ where } xn \equiv 0 \text{ or } 8 \pmod{10},$$

$$\text{or } p = xn - 1, \text{ where } xn \equiv 4 \text{ or } 8 \pmod{10}.$$

If n is odd, still more can be said. In the case $p \equiv 11$ or $19 \pmod{20}$ by theorem 5 we have $p-1=x.n$ for an integer x and $p-1=2y.n$ for no integer y , which is impossible for odd primes p . Similarly we reach a contradiction if $p \equiv 3$ or $7 \pmod{20}$. So, if n is odd, then $p = xn + 1$ where $xn \equiv 0$ or $8 \pmod{20}$, or $p = xn - 1$ where $xn \equiv 14$ or $18 \pmod{20}$, hence in each case $p \equiv 1 \pmod{4}$.

Remark 1. For odd n each prime factor p of u_n is a non trivial prime factor of u_m for some $m \mid n$, hence $\equiv 1 \pmod{4}$ (with the exception of $p=2$).

Remark 2. If n is odd, by (4) u_n is a sum of two squares, $a^2 + b^2$ say. If $p \equiv 3 \pmod{4}$ and $p \mid u_n$, then the number of factors p in u_n is even⁶). So if $p \equiv 3 \pmod{4}$ and $c(p)$ is odd, then $k(p)$ is even. We do not know prime numbers p for which $k(p) > 1$.

6) Confer Hardy and Wright, An introduction to the theory of numbers, theorem 366.

We give a table⁷⁾ of the values of $c(p)$, $C(p)$ and $v(p)$ for some primes p . In all these cases the value of $k(p)$ is found to be = 1

p	c	C	v	p	c	C	v
3	4	8	2	11	10	10	1
7	8	16	2	19	18	18	1
13	7	28	4	29	14	14	1
17	9	36	4	31	30	30	1
23	24	48	2	41	20	40	2
37	19	76	4	59	58	58	1
43	44	88	2	61	15	60	4
47	16	32	2	71	70	70	1
53	27	108	4	79	78	78	1
67	68	136	2	89	11	44	4
73	37	148	4	101	50	50	1
83	84	168	2	109	27	108	4
97	49	196	4	131	130	130	1
103	104	208	2	139	46	46	1
107	36	72	2	149	37	148	4
113	19	76	4	151	50	50	1
127	128	256	2	179	178	178	1
137	69	276	4	181	90	90	1
157	79	316	4	191	190	190	1
163	164	328	2	199	22	22	1
167	168	336	2	211	42	42	1
173	87	348	4	229	114	114	1
193	97	388	4	239	238	238	1
197	99	396	4	241	120	240	2
223	224	448	2	251	250	250	1
227	228	456	2	269	67	268	4
233	13	52	4	271	270	270	1
257	129	516	4	281	28	56	2
263	88	176	2	311	310	310	1
277	139	556	4	331	110	110	1
283	284	568	2	349	174	174	1
293	147	588	4	359	358	358	1
307	44	88	2	379	378	378	1
313	157	328	4	389	97	388	4
317	159	636	4	401	100	200	2
337	169	676	4	409	204	408	2
347	116	232	2	419	418	418	1
353	59	236	4	421	21	84	4
367	368	736	2	431	430	430	1
373	187	748	4				
383	384	768	2				
397	199	796	4				

7) Confer. D. Jarden, Table of the ranks of apparition in Fibonacci's sequence, Riveon Lemat.1(1946), 54.